INTELLIGENCE FUNDAMENTALS

INTERSCHOOL SUBCOURSE IS3002

EDITION C

2 CREDIT HOURS

June 2000

Prepared by

U.S. ARMY INTELLIGENCE CENTER

Fort Huachuca, AZ 85613-6000

SUBCOURSE OVERVIEW

This subcourse is designed to teach you intelligence fundamentals which involve the major elements of combat information and the intelligence cycle. It describes the phases of the intelligence cycle, processing of captured documents and personnel, counterintelligence (CI), collection methods, intelligence and training, safeguarding defense information, and military intelligence organization.

There are no prerequisites for this subcourse.

This subcourse reflects the doctrine which was current at the time the subcourse was prepared. In your own situation, always refer to the latest publications.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men.

Terminal Learning Objective:

Action: You will be able to identify the major elements of combat information, phases of the intelligence cycle, processing of captured enemy documents and materiel, counterintelligence, collection methods, intelligence and training, information security, and military intelligence organization.

Condition: You will be given narrative information from AR 380-5, JP 2-0, FM 34-1, FM 34-2-1, FM 34-3, FM 34-60, FM 34-80, and FM 34-130.

Standards: To demonstrate competency of this task, you must achieve a minimum of 70% on this subcourse examination.

TABLE OF CONTENTS

LESSON I

INTELLIGENCE FUNDAMENTALS

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn about intelligence fundamentals.

Terminal Learning Objective:

Tasks: You will be able to describe combat information and the intelligence cycle, how to handle enemy prisoners of war (EPW), and captured documents and materiel. You will also describe counterintelligence, collection methods, intelligence and training, safeguarding defense information, and military intelligence organization.

Conditions: You will be given narrative information and illustrations from AR 380-5, FM 34-1, FM 34-2-1, FM 34-3, FM 34-60, FM 34-80, and FM 34-130.

Standards: You will be able to understand intelligence fundamentals in accordance with the publications listed above.

References: The material contained in this lesson was derived from the following publications:

AR 380-5
FM 34-1
FM 34-2-1
FM 34-3
FM 34-60
FM 34-80
FM 34-130

INTRODUCTION

The importance combat information plays in mission accomplishment cannot be over-emphasized. As a result, everyone involved, regardless of military occupational specialty, should be aware of every major aspect of combat intelligence. This process will be used in both peacetime and wartime, but will be stressed more during a wartime situation.

PART A: INTELLIGENCE AND COMBAT INFORMATION

Intelligence operations are the wide-ranging activities conducted by intelligence staffs and organizations for the purpose of providing the commander with accurate and timely intelligence. Intelligence provides knowledge of the enemy to commanders enabling them to know what their adversary is doing, capable of doing, and what they will do in the future. Dominant battlespace awareness is one of the keys to warfighting. To achieve this, commanders must have the ability to collect, control, exploit, disseminate, and defend information while exploiting or denying the enemy's ability to do the same.

During war, intelligence strives to identify the enemy's capabilities, centers of gravity, project probable courses of action, and assist in planning friendly force employment. During stability and support operations (SASO), intelligence helps the commander decide which forces to deploy, when, how, and where to deploy them; and how to employ them in a manner that accomplishes the mission at the lowest human and political cost. Effective intelligence enables the commander to engage his forces wisely, efficiently, and effectively.

The commander is responsible for all intelligence activities of his unit. At battalion and brigade level, the commander demands the maximum effort from his intelligence officer (S2) in producing intelligence on enemy capabilities, and in determining the effects of those capabilities on the unit's mission, and on the operation plans prepared for the mission. The commander must counter the enemy's capabilities and accomplish his mission successfully. To assist him, the G2/S2 must answer the commander's questions on such subjects as strength, disposition, and identity of enemy units and the location of enemy weapons and defenses. The G2/S2 must also determine the enemy's capabilities and probable courses of action.

Combat information is that knowledge of the enemy situations, weather, and terrain features required by a commander in planning and conducting tactical operations.

The enemy situation is of prime importance to the commander in planning an operation. To assess this situation, the intelligence officer uses every available collection means to assemble information concerning the enemy's disposition, capabilities, vulnerabilities, and intentions. This analysis provides a comprehensive picture of the enemy situation.

The intelligence officer is also concerned with the command's requirements for weather information. He coordinates the collection and dissemination of weather data, interpreting them in terms of their effect on both friendly and enemy operations. He must also consider how the weather conditions will affect personnel, their equipment, and the terrain. For example, air operations in Vietnam were drastically reduced during periods of monsoon rains and early morning ground fog.

The intelligence officer analyzes terrain concerning five military aspects: observation and fields of fire, concealment and cover, obstacles, key terrain, and avenues of approach. For example, a hilltop between two valleys is considered key terrain. From it, a unit may achieve excellent observation of both valleys. If this hilltop is thickly vegetated and rocky, it offers the unit occupying it both concealment and cover. Similarly, such terrain is an obstacle for any enemy unit attempting either to pass through the valleys or to take the hill from the occupying force. Trails leading to the hilltop from the valleys, and the valleys themselves are possible avenues of approach for enemy forces. Because of the thick vegetation and rocks, fields of fire are generally poor. The intelligence officer provides the results of such an analysis to the commander in his intelligence estimate. Like weather, the terrain has an impact on both friendly and enemy courses of action.

The intelligence officer assembles all this information, interprets it in the light of other data available, and produces combat information--a thorough assessment of the enemy situation, the weather, and the terrain, which the commander can use as a basis for his decisions.

PART B: INTELLIGENCE CYCLE

The intelligence activities connected with the production of intelligence follow a process known as the "intelligence cycle." The intelligence cycle is the process by which information is converted into intelligence and made available for use in decision-making, planning, and execution. The cycle, previously five-phased, is now six-phased. The overarching principle of the cycle is intelligence synchronization. Each step within the cycle must be synchronized with the commander's decision making and operational requirements to successfully influence the outcome of the operation (see Figure 1-1). Remaining mission-focused is essential to successful intelligence operations. The intelligence cycle follows the following phases:

- Planning and direction.
- Collection.
- Processing and exploitation.
- Analysis and production.
- Dissemination and integration.
- Evaluation and feedback.

The intelligence cycle is a continuous process in which steps are executed concurrently, though not always sequentially. For example, while new information is being collected to satisfy one set of requirements, the G2 (S2), plans and redirects efforts to meet new demands while intelligence produced from previously collected information is disseminated. One or several iterations of the intelligence cycle may be conducted depending on the time constraints of the mission. The commander's mission provides the focal point for all phases of the cycle.

Planning and Directing

Intelligence preparation of the battlefield (IPB) is the primary task which helps the G2 (S2) focus and direct this step and the remaining steps of the intelligence cycle. Planning and directing involves task organizing MI assets; identifying personnel, logistics, and communications requirements; identifying, prioritizing, and validating intelligence requirements; developing a collection plan and synchronization matrix; issuing special order or requests (SORs) for collection and production; and monitoring the availability of collection information.

The intelligence officer must direct each collection operation to provide sufficient intelligence to meet the commander's requirements. However, the collection capabilities of a unit are rarely sufficient to satisfy all intelligence requirements simultaneously. Therefore, a system of commander's priorities is used to help the intelligence officer direct the available collection resources toward definite objectives. Requirements are classed either as priority intelligence requirements (PIR) or information requirements (IR).

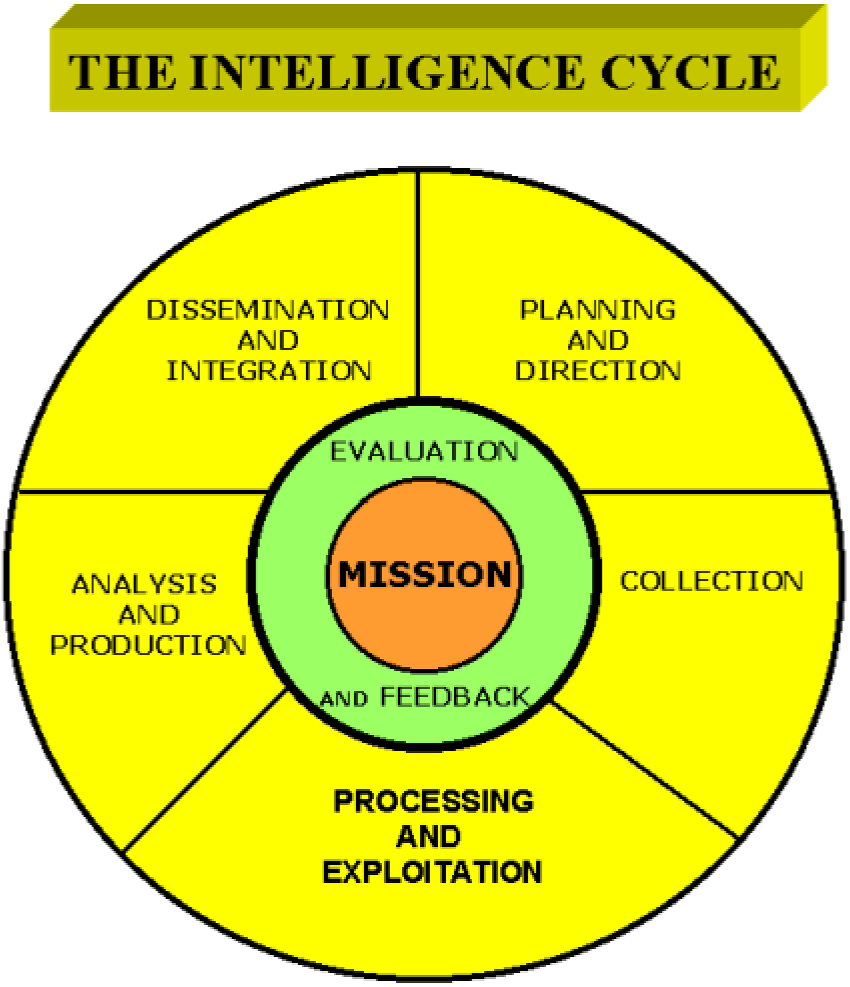

Figure 1-1. The Intelligence Cycle.

- PIRs are expressions of the commander's information needs. They reflect a dynamic thought process intended to seek answers to questions critical to the successful accomplishment of the unit's mission. The commander conveys his information needs to the G2/S2 who converts them into PIRs and IRs for the commander's approval or modification. PIRs can be an enemy capability, an enemy course of action, or characteristic of the battlefield which could decisively impact the commander's tactical decision. There is no prescribed limit to the number of PIRs that can be established. However, the number of PIRs should be minimized and phased with the concept of operation to better focus collection capability. Regardless of the number of PIRs developed, there should be a clear priority among them.

- IRs provide intelligence less critical to the commanders tactical decisions, as well as information to support the needs of other functional areas and subordinate units of the command.

The commander, through the G2 or S2, directs the intelligence effort. Based on knowledge of the enemy, weather, and terrain, the G2 or S2 develops intelligence requirements to support the commander's concept of operations.

Collection.

During the collection phase, intelligence sources identified in the collection plan collect information about the battlespace and adversary. The collected information is then provided to processing and exploitation elements. It includes the maneuver and positioning of intelligence assets to locations favorable to satisfying collection objectives.

Sources of information are persons, things, or actions from which enemy, weather, or terrain information is derived. Major sources include enemy activities, enemy communications, civilians, maps, weather forecasts, and studies prepared by higher, lower, and adjacent friendly units. Intelligence reports, such as shelling reports, imagery analysis reports, and crater reports, are also sources.

A collection agency is any individual, organization, or unit that has access to sources of information and the capability of collecting information from them. Collecting agencies include troops, intelligence specialists, and special units.

- Combat or combat support troops contribute information to the intelligence collection effort. The primary mission of a unit determines the amount of information that it can provide in this phase of the intelligence cycle. A rifle company, for example, because of its constant contact with the enemy, generally contributes more initial information on the enemy than most other types of units.
- Intelligence specialists are valuable collectors of information. Interrogators, imagery analysts, and CI specialists are typically such specially trained personnel. For example, the interrogator, by his direct contact with enemy prisoner of war (EPW), obtains valuable information from this primary source.
- Special units such as Special Forces and certain technical intelligence organizations have various specific collection missions significant to the overall collection effort these are usually missioned planned by the intelligence officer.

Processing and Exploitation Phase.

During this phase, raw collected information is converted into a suitable form that can be readily used by intelligence analysts in the production phase. Processing and exploitation actions include initial imagery interpretation, data conversion and correlation, document translation, and decryption. Processing and exploitation may be performed by the same agency that collected the information. Processing and exploitation could be taking technical parameters such as frequency, pulse repetition frequency, and bandwidth and associating the parameters with a particular radar system. Because of improvements in software and hardware, captured adversary documents may only require translating before they can be used by analysts.

The intelligence journal, intelligence workbook, and enemy situation map (SITMAP) are used as vehicles for recording pertinent intelligence information.

- The intelligence journal is a chronological log of intelligence activities covering a stated period, usually 24 hours. It is an index of reports and messages that have been received and transmitted, important events that have occurred, and actions taken. The journal is a permanent and official record. The commander may prescribe separate journals for the S2 and S3 staff sections or a single journal because of the increased dual functions of those sections.
- The intelligence workbook is a recording aid for sorting, evaluating, and interpreting information and for preparing intelligence reports. Recorded information is grouped by subject matter to simplify ready reference and comparison. The workbook is maintained by the S2 section personnel who make new entries and delete obsolete ones. It is not a permanent record, and it is not distributed to outside units or agencies.
- The enemy SITMAP is a temporary graphic record of the current disposition and major activities of the enemy. Information of friendly forces indicated on this map is usually limited to boundaries, locations of command posts of higher, lower, and adjacent units, reconnaissance units and the forward edge of the battle area (FEBA).

After the information is recorded, it is evaluted. The information is examined to determine its pertinence, reliability of the source and the collection agency, and accuracy of the information. Determinations might include: Does certain information apply to the current area of operations, and if so, to what extent? Is the information of value now, or will it be at a later date? How reliable are the source and the agency? For example, was the EPW lying or telling the truth, and how objectively did the interrogator obtain this information?

The last step in the processing and exploitation phase is interpretation based on study of the evaluated information. Analysis is made for possible indications of the enemy's intentions, general situation, capabilities, and vulnerabilities. At the same time, this information is compared with past intelligence. From this analysis and comparison probable conclusions are reached, and the collected information becomes intelligence.

Analysis and Production.

During this phase, all available processed information is integrated, analyzed, evaluated, and interpreted to create products that will satisfy the commander's PIR. Producing involves the integration, evaluation, analysis, and synthesis of information from single or multiple sources into intelligence. Activities during the analysis and production phase result in intelligence products. These products are placed in one of the following six categories:

- Indications and Warning (I&W). I&W intelligence concerns foreign developments that could involve a threat to the United States, US or allied military forces, US political or economic interests, or to US citizens abroad. I&W is time-sensitive and it includes forewarning of adversary actions or intentions.
- Current. Current intelligence provides updated support for ongoing operations. It involves the integration of time-sensitive, all-source intelligence and information into concise, objective reporting on the current situation in a particular area.

- General military. This involves intelligence concerning the military capabilities of foreign countries and organizations and other topics that could affect potential US or allied military operations.
- Target.
- Scientific and technical.
- CI. The categories are distinguished from each other by the purpose each product was intended for. Products can and often do overlap into different categories. At the tactical level, time constraints and demands of the battle tend to make the processing and exploitation phase and the analysis and production phase indistinguishable.

Dissemination and Integration.

During this phase, intelligence is delivered to and used by the consumer. Disseminating intelligence is the timely conveyance of intelligence to users in a usable form. The diversity of forms and means requires interoperability among command, control, communications, and intelligence (C^3I) systems. The most valuable information or intelligence is worthless unless it is disseminated to the appropriate users in time for them to exploit it and in a form that can be clearly understood. First priority is given to the commander. Distribution is also made to staff personnel and to higher, lower, and adjacent units most concerned with, or affected by, the information.

The method of dissemination used varies with the importance and timeliness of each item of intelligence. Basic means of dissemination include messages (radio or other rapid means of signal communications), personal contact (telephone, briefings, and personal visits), intelligence documents (intelligence estimates, operations orders, and intelligence annexes) periodic reports, analysis of the area of operations, "as required" reports, and studies. The diversity of dissemination paths reinforces the need for interoperability among command, control, communications, computers, and intelligence.

Intelligence organizations at all levels must ensure that their products are getting to the users by the time they are needed. Intelligence organizations must initiate and maintain close contact with the user to ensure that the product has been received. Intelligence personnel will be relied upon to support the decision-making and planning processes. Products may require further clarification or they may raise new issues that must be immediately addressed. Integration is a continuous dialogue between the user and the producer.

Evaluation and Feedback

During the last phase, intelligence personnel at all levels assess how well each phase of the intelligence cycle is being performed. Commanders and operational staff elements must provide feedback. When areas are identified that need improvement, changes are implemented.

PART C: HANDLING EPW, CAPTURED ENEMY DOCUMENTS, AND MATERIEL

EPWs, captured enemy documents, and materiel are primary sources of information concerning the enemy. Thus, they must be properly and effectively handled to maximize their value to the collection effort.

EPWs are disarmed and thoroughly searched immediately after capture, as they often have concealed weapons or documents on them. As soon as practical, they are segregated and individually interrogated. The capturing unit stresses questions of immediate tactical importance during this initial and normally brief interrogation. After they have been properly tagged, EPWs are evacuated as soon as possible to higher headquarters for further and more detailed interrogation. At division level and above, emphasis is placed on questions of strategic as well as tactical significance.

Captured enemy documents (CEDs) are examined briefly for information of immediate tactical importance to the capturing unit. After being properly tagged, the documents are forwarded without delay to higher headquarters so the intelligence value of the documents may be exploited at the earliest possible time.

Captured enemy materials (CEMs) like captured documents, are tagged and forwarded to higher headquarters without delay. Documents relating to the technical design or operation of the captured materiel or equipment should accompany it whenever possible. However, if operational circumstances or the size of the materiel prohibits shipment of the object itself, the documents should be evacuated separately through intelligence channels. These documents are identified with the captured materiel by the use of an attached sheet, marked technical document, which lists the precise location, time, and circumstances of capture, and as detailed a description as possible of the materiel or equipment. Whenever possible, photographs should be taken of the materiel and sent forward with the documents.

NOTE: CEMs also includes weapons.

All CEDs or devices dealing with codes, ciphers, or crypto-material of any kind, will be treated as SECRET matter and evacuated by the most expeditious means through intelligence channels.

Capturing units should tag all EPW, CEDs, and CEMs with the following minimum information before evacuation to higher headquarters:

- Date and time of capture.
- Location of capture.
- Circumstances of capture.
- Capturing unit.

PART D: COUNTERINTELLIGENCE (CI)

As part of his intelligence responsibilities, the intelligence officer exercises staff supervision over all CI within his unit. He implements and supervises CI measures directed by higher headquarters and is the staff advisor for the application of CI measures in any operational situation of his unit.

Three types of measures employed in CI operations are denial, detection, and deception of threat intelligence collection efforts.

- Denial measures are used to prevent the enemy from obtaining information. Methods of denial include document security, physical security of installations, signal communication security, censorship, and counterreconnaissance (CR). For example, by ensuring classified documents are properly stored and secured, we deny the enemy access to potentially valuable sources of information.

- Detection measures are designed to expose and neutralize the enemy intelligence effort. Checkpoints operated by battalion and brigade-size units to control the movement of vehicles and personnel in their area of operations are typical of this CI measure. Conducting checks enables such units to apprehend enemy agents or sympathizers possessing faulty identification or war materiel (for example, guns, ammunition, and explosives).
- Deception is the use of measures to mislead the enemy concerning the status or purpose of friendly activities, personnel, weapons strength and disposition, and logistical buildup. Feints, ruses, and the leaking of false information to the enemy are examples of deception. Normally, deception activities of this type are initiated, directed, and controlled by higher headquarters. Deception measures originating at a lower echelon must be approved by higher headquarters. While the S2 provides recommendations and the necessary intelligence support and coordination for deception measures, the S3 has staff responsibility for actually implementing these activities.

CI measures can be either offensive or defensive in nature.

- Offensive CI measures actively block the enemy's attempts to gain information or by engaging in sabotage or subversion. A combat patrol capturing an enemy agent behind enemy lines is an example of an offensive CI operation.
- Defensive CI measures, on the other hand, are attempts to conceal information from the enemy. Secrecy discipline, security of classified documents and materials, signal security, and censorship are examples of defensive CI measures and they are usually standardized in unit standing operating procedures (SOP).

The essence of the Army's CI mission is to support force protection. By its nature, CI is a multidiscipline (C-HUMINT, C-SIGINT, and C-IMINT) function designed to degrade threat intelligence and targeting capabilities. Multidiscipline counterintelligence (MDCI) is an integral and equal part of intelligence and electronic warfare (IEW). MDCI operations support force protection through operations security (OPSEC), deception, and rear area operations across the range of military operations.

CI must meet the goals and objectives of Force XXI and force projection operations. US Forces will be continental United States (CONUS)-based with a limited forward presence. The Army must be capable of rapidly deploying anywhere in the world; operating in a joint or combined (multinational) environment; defeating simultaneous regional threats on the battlefield; or conducting stability and support operations (SASO). CI, as part of IEW, is fundamental to effective planning, security, and execution of force projection operations. CI, in support of force protection, will be required on the initial deployment of any force projection operation.

The commander focuses on the intelligence system by clearly designating his priority intelligence requirements (PIR), targeting requirements and priorities. He ensures that the Intelligence Battlefield Operating System (BOS) is fully employed and synchronized with his maneuver and fire support BOS. He demands that the Intelligence BOS provides the intelligence he needs, when he needs it, and in the form he needs.

The G2 synchronizes intelligence collection, analysis, and dissemination with operations to ensure the commander receives the intelligence he needs, in the form he can use, and in time to influence the decision-making process. Intelligence is a continuous process which keeps IEW operations tied to the commander's critical decisions and concept of operations. CI collection, analysis, and dissemination, like other intelligence, have to meet the commander's time requirements to be of any use other than historical.

The role of CI is to support the commander's requirements to preserve essential secrecy and to protect the force directly or indirectly. Thus, CI contributes to the commander's force protection programs. Force protection is a command responsibility to protect personnel, equipment, and facilities. To carry out his force protection responsibilities, a commander requires support from several sources, one of which is the intelligence community. CI support to force protection must be tailored to the sensitivity of the supported organization and its vulnerability to foreign intelligence service (FIS) and hostile attack. CI support can be tailored from a combination of activities to include:

- Mobilization security, including ports and major records repositories.
- Combating terrorism.
- Rear operations.
- Civil-military affairs.
- Psychological operations (PSYOP).
- Battlefield deception.
- OPSEC.
- Friendly Communications-Electronics (C-E) (C-SIGINT).
- CI force protection source operations (CFSO).

Army CI is not limited to the activities of a small force of CI agents and technicians; rather, it is the responsibility of all Army personnel to follow common sense security measures to minimize any foreign intelligence threat.

Although a major part of the CI mission is to counter or neutralize FIS efforts, this does not mean that only CI personnel take part in these actions. They may require:

- Other intelligence specialists such as interrogators.
- Military police (MP).
- Civilian counterparts and authorities.
- Combat forces.
- Civil-military affairs and PSYOP.
- Criminal Investigation Command (CIDC) agents.

CI is that phase of intelligence activity aimed at destroying the effectiveness of enemy foreign intelligence activities, and at protecting information against espionage, personnel against subversion, and installations or materiel against sabotage.

PART E: RECONNAISSANCE AND SURVEILLANCE (R&S)

Effective ground and aerial R&S measures make essential contributions to the intelligence collection efforts of any unit. Combat surveillance is defined as the continuous, all-weather, day-and-night, systematic watch over the battlefield area to provide timely information for tactical ground combat operations. There are several standard combat surveillance means available to the command, including the following: personnel (reconnaissance patrols, forward observers, aerial observers, and observation posts), specially trained units (long-range reconnaissance patrols), and devices (optical instruments, battlefield illumination, aircraft, cameras, radar, infrared techniques, magnetic and radio instruments, chemical detector kits, and sound detection devices).

Reconnaissance is concerned with three components: enemy, weather, and terrain. You should understand that reconnaissance is active; it seeks out enemy positions, obstacles, and routes. Since movement draws attention, good reconnaissance uses stealth to avoid detection.

Surveillance is passive. Surveillance implies observing a specified area or areas systematically from a fixed, concealed position. A good R&S plan contains the best mix of R&S based on requirements, assets available, and the threat.

Then plan how to find the enemy's reconnaissance assets before they are able to find friendly forces. You also need to understand US maneuver organizations, doctrine, tactics, and capabilities, since you may be called on to provide a recommendation for organizing CR forces.

Defining R&S and counterreconnaissance in isolation may suggest they occur in a vacuum.

Nothing could be further from the truth. R&S is a crucial phase of the intelligence cycle. As you will see, your R&S effort requires direction if it is to provide the necessary intelligence the commander needs to fight and win the battle.

You might have the impression R&S has definitive start and end points. Actually, R&S is part of a larger, continuing collection process. That process gets its direction from two things: first, the mission; and second, by extension, the intelligence preparation of the battlefieId (IPB) process. These two things tell you--

- What to collect.
- Where to collect.
- When to collect.
- Who should collect it for you.
- Why you must collect it.

Your collection plan enables you to direct and control the collection of information. That information, once recorded, evaluated, and interpreted, becomes intelligence. Collecting information gives commanders targeting data so they can destroy enemy weapon systems and units. Your analysis can provide insight into the enemy situation to the extent that you can make an educated estimate of possible future enemy courses of action (COAs). At this point, inform your commander and the rest of the staff; then begin to develop friendly COAs for future operations.

The cycle continues endlessly. However, within the cycle you may discover, based on the picture you have developed, that you must modify the collection plan. Or, based on what you have collected, you must update the IPB terrain data base.

There is an interrelationship between all aspects of the intelligence cycle. Your collection plan has a direct effect on how you--

- Process information and disseminate intelligence during the present battle.
- Direct your intelligence efforts for future battles.

The R&S plan marries the IPB with assets available for information collection. It organizes and prioritizes information requirements. This results in R&S taskings to units through the S3.

Two principles of R&S are:

- Tell commanders what they need to know in time for them to act. This principle is of paramount importance. You must develop the R&S plan so that it directly addresses what the commander wants to know. In essence, the R&S effort (as with the intelligence effort in general) is commander-oriented and commander-directed. Therefore, you cannot develop a successful R&S plan until you know exactly what the commander needs to know.
- The commander's questions which absolutely must be answered in order to accomplish the mission are PIR. They are the start point for the R&S plan. The clearer and more precise the commander's PIR, the better you will be able to develop the R&S plan to answer them.

How do PIR come about? As part of the mission analysis process, you and your commander study the mission given to you by higher headquarters. You develop specified, implied, and essential tasks. As you do this, you should also be able to identify gaps in your understanding of the battlefield situation.

Remember, PIR drive your R&S efforts; so it is critical that you understand just exactly what your commander needs to know in order to fight. To better focus R&S efforts, keep PIR down to a manageable number. Normally, you will only be able to concentrate on three or four at any one time. Of course, the mission and the commander's needs may sometimes dictate more. Having a large number of priorities defeats the purpose of having PIR in the first place.

Since R&S activities contribute directly to the commander's information collection effort, planning for R&S activities occurs concurrently with collection planning to ensure a fully integrated, comprehensive collection effort. Thus, the intelligence officer must plan the systematic watch of the battlefield area, coordinate and integrate all surveillance activities, assign mission priorities for surveillance, develop intelligence from the information subsequently acquired, and furnish the resultant intelligence to users.

Throughout R&S planning, the intelligence officer must coordinate closely with the S3, who provides him with continuous information on current friendly troop locations, activities, and plans, and designates the combat units to be used in support of R&S missions. Such coordination ensures R&S activities support the unit's primary mission.

PART F: MAP AND PHOTO ACTIVITIES

The intelligence officer is responsible for obtaining all maps needed by his unit. This involves planning ahead for the map requirements, then directing and coordinating all map activities of the command to include the procurement, production, reproduction, storage, and distribution of maps and map substitutes. He must coordinate closely with the logistical officer for the procurement of the maps and their subsequent storage and distribution, and with the engineer officer who has special staff responsibility for the production and reproduction of maps and map substitutes.

In conjunction with his map responsibilities, the intelligence officer also plans for and supervises all aerial photographic activities. He must determine the needs of his unit, request the needed aerial photography, and then use either the imagery readout or aerial photography in compiling intelligence on a given area.

PART G: TARGETING

Targeting is an assessment of the terrain and threat that identifies enemy formations, equipment, facilities, and terrain which must be attacked to ensure friendly success. It is based on the friendly concept of the operation, scheme of maneuver, or tactical plan.

It begins with the commander's guidance and continues through the development of a prioritized list of what targets are to be attacked, when they are to be attacked, and what is required to defeat them.

Targeting is a staff function accomplished primarily by the operations officer (S3), the intelligence officer (S2), and the fire support element (FSE), also known as the targeting team. As required, or as directed by the commander, other staff members may augment the team to enhance the targeting process.

The intelligence officer's targeting responsibilities involve the following:

- Predicting probable and most likely enemy courses of action based on an analysis of the battlefield area and IPB.
- Conducting coordination within the targeting team in order to determine what elements of the enemy force are most critical to its success, that is, which elements are the most "valuable" targets, and compile a high value target (HVT) list.
- Tasking sensor systems necessary to support the targeting process through proper collection planning and collection management.

All sensors or collection assets must be considered to include those assets available to subordinate, higher, adjacent, and cooperating units.

Some examples of sensors or collection assets available to the intelligence officer include:

- Forward observers.
- Observation posts.
- Counter mortar/counter battery radar.
- Aerial observers.
- Imagery intelligence (IMINT).
- Signals intelligence (SIGINT).
- Ground surveillance radars.
- Maneuver Units.
- Designating protected targets (those targets which might best be exploited by intelligence assets, that is, SIGINT, which comprises all communications intelligence (COMINT) electronic

intelligence (ELINT), and telemetry intelligence (TELINT) and once approved by the commander, coordinating these targets with the appropriate intelligence agencies/functions.)

PART H: NUCLEAR, CHEMICAL, BIOLOGICAL ACTIVITIES

In coordination with other staff officers, the S2 processes and disseminates intelligence on enemy nuclear, biological, and chemical resources and capabilities. He also reviews the chemical officer's plans for the prediction of enemy-delivered nuclear weapons fallout, detection of chemical and biological agents, radiological monitoring, and survey operations to ensure these plans support the unit's mission.

The intelligence officer further ensures procedures and communications are available for the collection, evaluation, and dissemination of information concerning fallout from enemy-delivered weapons, and for all detection, monitoring, and survey operations. He determines the probable effects of fallout from enemy-delivered weapons on the area of operations, friendly operations, and enemy capabilities, and provides estimates concerning this information to the commander and other appropriate staff officers for their use in planning.

The intelligence officer continually coordinates with the operations officer to ensure the responsibilities of the S2 for the prediction and dissemination of information on fallout from enemy-delivered weapons, and of the S3 for the prediction and dissemination of information on fallout from friendly delivered weapons, are completed with minimum conflict of interest or duplication of effort.

PART I: INTELLIGENCE AND TRAINING

Each soldier is a potential information collection agency. In such a capacity his duties would be to observe and report. He reports what he sees, where he sees it, and when he sees it, to his immediate commander or leader. Before the soldier can be expected to make such reports, however, he must be trained to observe and learn what to report and how to report it. He must be made aware of the vital importance of his front-line reports to the success of his units' mission. Intelligence reporting is not second nature to the untrained soldier. During battle he is fully occupied with his primary job, whether he is a rifleman, machine gunner, ammunition bearer, radio operator, or wireman. Unless he has been thoroughly trained and indoctrinated, he may not observe or report many items of valuable information.

The primary objective of intelligence training is to develop intelligence consciousness in each soldier. The efficient performance of a command's intelligence functions depends largely upon how well such intelligence consciousness is created and maintained by all individuals in the command. Intelligence training must develop in each soldier an awareness of his role in the production of combat information and its significance to his unit and him. Such training is continuous and will pay prompt and usable dividends in combat. The results of careless or insufficient intelligence training will appear just as quickly in combat.

The ultimate goal of intelligence training is to make observing and reporting information a habit with each soldier, whether he is a rifleman, clerk-typist, medic, or cook. Football players spend long grueling hours learning how to block. Later, in the heat and rush of the game, blocking is an accurate and automatic reflex action. The same principle applies to training in observing and reporting information. There must be an automatic reflex action on the part of each soldier to ensure he accurately and automatically reports all information observed no matter how small or insignificant it may appear to be.

The intelligence officer exercises staff supervision over all intelligence and CI training within the command. In fulfilling this responsibility, the S2 prepares training programs (including the preparation of realistic training exercises to supplement classroom and other intelligence instruction), conducts intelligence training programs, supervises intelligence training, conducts tests, and assists subordinate units in obtaining training aids and qualified instructors. He coordinates closely with the operations officer, who is responsible for overall training in the unit, other staff officers, and individual unit commanders within the command. This ensures the integration of intelligence training programs throughout the unit. Throughout this supervision and coordination, the intelligence officer attempts to accomplish his primary training goal: the development of intelligence consciousness in each soldier.

Some of the most common intelligence subjects stressed in intelligence training are the intelligence cycle and the role of the troops in the cycle, collecting and reporting information, observation, and handling EPW, enemy deserters, civilians, evaders, escapees, and captured documents.

CI subjects are also stressed in intelligence training. While every soldier is an excellent potential information-gathering agency for the intelligence officer, he is also a potential major source of information for the enemy. He must be adequately trained in basic CI areas. Two of the most common of these subject areas are communications security and safeguarding of defense information.

PART J: SAFEGUARDING DEFENSE INFORMATION

Defense information is "official information which requires protection in the interest of national defense, which is not common knowledge, and which would be of intelligence value to an enemy or potential enemy in the planning or waging of war against the United States." Information of such a sensitive nature must be adequately safeguarded.

Defense information is of varying degrees of value to foreign governments and enemy forces. It must be examined and evaluated by each individual who produces it. If the unauthorized disclosure of this information could be injurious to the defense interest of the nation, this information will be classified according to the degree of protection necessary for its safeguarding. Defense information is classified as either TOP SECRET, SECRET, or CONFIDENTIAL.

Defense information classified as TOP SECRET requires the highest degree of protection. The TOP SECRET classification is applied only to that information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the nation.

The SECRET classification is applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the nation.

The CONFIDENTIAL classification is applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause damage to the nation.

Each item of information in a given classified category must be marked, stored, transmitted, declassified, and destroyed according to procedures and requirements set forth in AR 380-5 pertaining to the safeguarding of defense information.

Classified information is strictly controlled, and before an individual is allowed access to such information, he must meet both of two rigid requirements. He must have the proper security clearance, and he must have a valid "need-to-know."

Security clearances are granted only after a favorable personnel security investigation has been conducted on the individual. The completed certificate of clearance (DA Form 873) authorizes access to defense information up to a specific classification. For example, an individual granted a SECRET clearance can also have access to CONFIDENTIAL defense information, but not TOP SECRET.

In addition to a security clearance, an individual must also demonstrate an official "need-to-know," that is, the nature of his duties must require he have access to the specific information concerned.

PART K: MILITARY INTELLIGENCE ORGANIZATION

The military intelligence (MI) organization consists of all personnel and units, along with administrative, logistical, and other support personnel required to provide intelligence and intelligence specialist support to the Theater Army. The MI specialists in this organization include EPW interrogators, imagery analysts, order of battle personnel, CI personnel, technical intelligence coordinators, strategic intelligence editors, and censors. These specialized intelligence personnel are organized into MI platoons, detachments, companies, battalions, and groups to meet the needs and requirements of the supported command.

The commander of the supported unit assumes operational control of the MI unit or element assigned or attached to his command. The intelligence staff officer (G2/S2) of the supported unit assigns requirements to the supporting MI unit in the name of the commander, maintains staff supervision over the MI unit, and furnishes appropriate guidance to it. All intelligence staff officers (G2/S2) of tactical commands maintain liaison with the supporting MI battalion or detachment commander to ensure timely and effective specialist intelligence support to their units.

MI specialists may be assigned to all levels from battalion to division within tactical commands.

Practice Exercise
Lesson 1

Instructions The following items will test your understanding of the material covered in this lesson. There is only one correct answer for each item. When you have completed the exercise, check your answers. If you answer any item incorrectlly, review that part of the lesson which contains the portion involved.

1. As an intelligence officer, which devices should you NOT use as a basic recording device?

   ○ A. Enemy situation map.

   B. Intelligence workbook.

   C. Intelligence journal.

   D. Intelligence summary.

2. What is the last phase of the intelligence cycle?

   A. Evaluation.

   B. Analysis and Production.

   C. Collection.

   D. Evaluation and feedback.

3. What is the primary objective of intelligence training?

   A. Develop intelligence consciousness in each soldier.

   B. Instill realism in training.

   C. Create an enemy situation.

   D. Teach from past mistakes.

4. PIRs are necessary for all of the following reasons except:

   A. PIRs are prioritized, phased, and minimized to focus collection capabilities.

   B. PIRs are expressions of the commander's information needs.

   C. It is not necessary for the G2/S2 to have the final approval for PIRs from the commander.

   D. PIRs can decisively impact the commander's tactical decisions.

5. Who is given priority for dissemination of intelligence?

   A. Commander.

   B. Staff.

   C. Higher headquarters.

   D. Front-line units.

6. The SECRET classification is applied only to:
   A. Information or material which the unauthorized disclosure could reasonably be expected to cause serious damage to the nation.
   B. Information or material the unauthorized disclosure of which reasonably could be expected to cause damage to the nation.
   C. Information that the classifying official doesn't want anyone else to see.
   D. Information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the nation.

7. Which counterintelligence measure governs the use of a checkpoint to control movement of personnel?
   A. Denial.

   B. Detection.

   C. Deception.

   D. Defensive.

8. Who provides the S2 with friendly information?
   A. The S3

   B. The FSE.

   C. The G2.

   D. The commander.

9. What are the primary sources of information concerning the enemy?
   A. EPW.

   B. EPW, CEDs, and CEMs.

   C. Enemy operations orders.

   D. Abandoned equipment, EPW.

10. Which staff officer is responsible for obtaining all maps needed by the unit?
   A. Logistics officer.

   B. Training officer.

   C. Intelligence officer.

   D. Operations officer.

Appendix A

GLOSSARY

Intelligence Terms

Combat Information -- That knowledge of the enemy situation, weather, and terrain required by a commander in the planning and conducting of tactical operations.

Counterintelligence -- That aspect of intelligence activity devoted to destroying the effectiveness of enemy foreign intelligence activities and protecting information against espionage, individuals against subversion, and installations or materiel against sabotage.

Deception -- CI measures designed to mislead the enemy by manipulating, distorting, or falsifying evidence to induce it to react in a manner prejudicial to its interests.

Denial -- CI measures used to prevent the enemy from obtaining information or producing intelligence about friendly forces.

Detection -- CI measures designed to expose and neutralize the enemy intelligence effort.

Espionage -- Actions directed toward the acquisition of information through clandestine operations.

Imagery Analyst -- An intelligence specialist qualified to recognize, identify, locate, describe, and analyze objects, activities, and terrain represented on imagery, and to extract intelligence information there from.

Imagery -- The representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media.

Information Requirements -- Information required by the commander or his staff to make sound decisions, but of second priority to priority intelligence requirements.

Intelligence -- The product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information which concerns one or more aspects of foreign nations or of areas of operations and which is immediately or potentially significant to military planning and operations.

Intelligence Annex -- A supporting document of an operations plan or order which provides detailed information on the enemy situation, assignment of intelligence tasks, and intelligence administrative procedures.

Intelligence Cycle -- The steps by which information is assembled, converted into intelligence, and made available to users. These steps are in five phases: plan and direct, collect, process, produce, and disseminate.

Intelligence Journal -- A chronological log of intelligence activities covering a stated period, usually 24 hours. It is a permanent and official record of reports and messages received and transmitted, important events, and actions taken.

Intelligence Officer -- The staff officer who assists the commander in fulfilling his intelligence responsibilities by supervising all intelligence and CI activities of the unit. At brigade and battalion the intelligence officer is the S2 on the special staff; at division is the G2 and all echelon above is the J2 on the joint staff.

Intelligence Specialists -- Personnel specifically trained to perform functions in the collection or processing of intelligence.

Intelligence Summary -- A specific report providing a summary of items of intelligence information normally produced at battalion/squadron, or higher level in tactical operations, usually at six-hour intervals.

Intelligence Workbook -- A recording aid for sorting, evaluating, and interpreting information and preparing intelligence reports. Information is grouped by subject matter and continually updated. The intelligence workbook is not a permanent record nor is it distributed to outside units or agencies.

Military Intelligence Organization -- Tables of Organization and Equipment units which provide intelligence specialist support to augment organic assets of the intelligence section from field army down to separate brigade or armored cavalry regiment level.

Order of Battle -- The identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force.

Periodic Intelligence Report -- A summary of intelligence information normally prepared at corps level or higher, and at 24-hour intervals.

Personnel Security Investigation -- A prerequisite to granting a security clearance. The extent of the investigation is dependent upon the individual's personal situation and the level of security clearance desired.

Priority Intelligence Requirements -- The critical items of information regarding the enemy and its environment required in order to make timely decisions.

Reconnaissance -- A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or about the characteristics of a particular area.

Sabotage -- An act with an intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring, destroying or attempting to injure or destroy any national defense or war materiel, premises, or utilities.

Sedition -- Willful making or conveying of reports or statements with the intent to interfere with the operation or the success of the United States armed forces or to promote the success of its enemies; the willful causing of insubordination, disloyalty, mutiny or refusal of duty in the armed forces, or willful obstruction of recruiting or enlistment service of the United States.

Strategic Intelligence -- Intelligence required for the formation of policy and military plans at national and international levels.

Subversion -- Action designed to undermine the military, economic, psychological, moral, or political strength of a regime.

Surveillance -- The systematic observation of aerospace, surface or subsurface areas, places, persons, or things by visual, aerial, electronic, photographic, or other means for intelligence purposes.

Target Acquisition -- The detection, identification, and location of a target in sufficient detail to permit the effective use of weapons.

Target Development -- The acquisition of targets through the analysis and correlation of information from all collection means; also called indirect target acquisition.

Technical Intelligence -- Intelligence concerning foreign technological developments, performance, and operational capabilities of foreign materiel which has or may have a practical application for military purposes.